# Oracle Database Vault

Frequently asked questions

April, 2025 Version 23ai

ORACLE

## Table of contents

# Overview

Oracle Database Vault prevents unauthorized privileged user access to sensitive data and unauthorized changes to the database through strong controls and enforced separation of duties. Database Vault allows you to limit when, where, and how database credentials are used by controlling their connect privilege. Database Vault can reduce the impact destructive commands (e.g., DROP TABLE, TRUNCATE TABLE) can have on your production data. Database Vault provides a powerful and transparent security solution that helps organizations comply with regulations, deploy systems cost-efficiently, and prevent unauthorized access to sensitive data.

# Features

## What does Oracle Database Vault do?

Oracle Database Vault provides strong security controls to prevent unauthorized access to sensitive information by privileged users, protect application schema credentials from misuse or abuse, and protect against unintended changes to the database. This reduces the risk of malicious users using privileged accounts to attack the database.

## Why do I need Oracle Database Vault if I already encrypt my database?

Most cyber-attacks use simple techniques to steal information. The most common method is to use stolen application schemas accounts or privileged user accounts. These accounts give the keys to the kingdom and allow cyber attackers to jump to parallel systems or exfiltrate data from a system.

Encryption prevents database bypass attacks, which can allow an attacker to steal sensitive data from database files at the OS level, storage devices, backup devices, and export files.

With proper encryption, cyber attackers are forced to attempt to attack the data by misusing or abusing privileged database user accounts to steal sensitive data from a database.  Enforcing strong controls with Oracle Database Vault minimizes the risk of a breach from the malicious use of privileged accounts.

Oracle Database Vault can control how database application schema accounts and privileged database user credentials can be used. For example, you can limit where, when, or how the database application schema account (e.g., HR) can be used to connect to the Oracle Database. This is an example of creating a trusted path for the application, or privileged database user, of connecting by restricting them to certain IP addresses or IP ranges, hostnames, time of day, day of the week, or restricting the client program or module they use to connect.

In addition to strong protection and access controls, Oracle Database Vault enforces and supports the separation of duty principles.

## How does Oracle Database Vault improve security and improve compliance?

Oracle Database Vault improves security by minimizing risks from privileged user attacks, the most common form of cyber-attack.  Most compliance requirements include controls for separation of duty and preventing administrative access to sensitive data. Since Oracle Database Vault implements security in the kernel of the database, these security controls are in place no matter what network or server the cyberattack originates from.

## Has Oracle Database Vault been evaluated against any security standard?

Oracle Database Vault has been certified with Common Criteria. Please review the Oracle Technology Network website for the latest information regarding Oracle Database and Database Vault certifications. The Common Criteria for IT Security Evaluations is an internationally recognized standard (ISO 15408) to measure the security of IT products.

## What security does Oracle Database Vault provide in the Cloud?

Oracle Database Vault protects sensitive data in a Cloud from attacks by cloud or customer administrators that have privileged user access to the database. The database is also protected from unauthorized changes by either cloud or customer administrators.

Oracle Database Vault is available to customers of Oracle Autonomous Database, Oracle Database Base Cloud Services (DBCS), ExaCS and ExaCC customers either as part of their license or an additional license.

## Can I use Oracle Database Vault to meet compliance requirements found in Sarbanes-Oxley, PCI, HIPAA, ITAR, and EU GDPR?

Oracle Database Vault is designed to help address technical security requirements found in various regulations such as Sarbanes-Oxley, PCI, HIPAA, ITAR, and EU GDPR. Customers are also required to follow processes and procedures required by these regulations. Oracle Database Vault provides strong internal controls inside the database controlling who, when, where, and how applications data can be accessed. In addition, Oracle Database Vault controls what changes can be made to the database helping keep the database available and secure.

# ADMINISTRATION

# Components and Features

## How do I install Oracle Database Vault?

Oracle Database Vault is built into the kernel of the Oracle Database. There is no agent or additional software to install. You simply create the users for Oracle Database Vault to use, configure Oracle Database Vault, and enable it in your container database and any or all of your pluggable databases.

## What security controls does Oracle Database Vault provide?

*Realms* - A realm is a "protection zone" inside the database that prevents privileged users such as DBAs from accessing any protected data inside it. The Oracle Database Vault security administrator can create a realm, add the sensitive database objects to be secured in it, and authorize the users or roles that need access to it. A realm can protect a single table, multiple tables, an entire application schema, or multiple application schemas. There is also a second type of realm called mandatory realms, where protection is extended to block unauthorized access even by object owners. Only a user assigned the appropriate Oracle Database Vault security role can authorize access to the sensitive data.

*Command rules* - A command rule controls the conditions under which users can execute any SQL statements, including SELECT, ALTER SYSTEM, database definition language (DDL) statements, and data manipulation language (DML) statements. Command rules evaluate a security policy (rule set) to determine whether or not the statement is allowed and under which conditions.

*Secure application roles* - Regular Oracle Database secure application roles are enabled by custom PL/SQL procedures. Secure application roles use Oracle Database Vault rules and rule sets to prevent users from accessing data from outside an application. This forces users to work within the framework of the application privileges that have been granted to the role.

*Operations control* – Operations control strengthens security for the popular database consolidation technology, Oracle Multitenant. Apart from using PDB lockdown profiles that prevent PDB users from affecting other PDBs and the database, Oracle Database Vault operations control transparently prevent Multitenant container administrators from accessing application data in pluggable databases.

*Authorizations* - Oracle Database Vault further limits privileged users by requiring them to be authorized to specific roles or privileges. For example, in Oracle Database 23ai, users with the AUDIT_ADMIN or AUDIT_VIEWER role must also be authorized by Oracle Database Vault to use their granted role(s). This ensures that even privileged users, who may be granted the role by default or by accident, cannot view or modify audit-related objects without the specific authorization to do so. Similar authorization is required to use Oracle Data Pump, proxy authentication, and more.

## What new roles are created for Database Vault?

Database Vault creates several roles to help you enforce separation of duties within the Oracle Database, including DV_MONITOR for DBSNMP and DV_SECANALYST for reporting on specific SYS and Database Vault-related views. For more information on these views and others, please see the Oracle Database Vault Administrator's Guide documentation.

Two primary roles are created and granted to users when Oracle Database Vault is created. They are DV_OWNER and DV_ACCTMGR roles. The DV_OWNER role allows the user to create security objects (realms, command rules, etc.), add authorized users, enable/disable controls, and perform other management tasks related to the Database Vault security objects. DV_ACCTMGR role is used to create and manage users and profiles. It is important to note that backup accounts are recommended for these two roles since no other database privilege, including SYSDBA, will be able to recover lost passwords for accounts with these roles. In other words, at least two database accounts should have the DV_OWNER role with admin option– one or more used for day-to-day configuration and management of Database Vault, another as an emergency account stored in your organization's privileged account management solution.

## Do the new Oracle Database Vault roles change how my database administrators work today?

Most DBA tasks will not change. Most organizations want to limit administrative staff from viewing sensitive data. As most of your day-to-day DBA tasks do not require direct access to protected data, Database Vault allows your administrators to continue to perform these tasks.

You will notice one area of change is creating and managing users and profiles. This security-related task can only be done by a user with the DV_ACCTMGR role. You are welcome to grant this role to any user who performs user or profile management as part of their duties. Additionally, tasks that can expose sensitive data, like Oracle Data Pump and Job Scheduling, need separate authorization from an account with the DV_OWNER role.

Oracle recommends you take advantage of the different roles and assign them to named user accounts (e.g. JSMITH) instead of continuing to use shared accounts (e.g. SYS or SYSTEM) to perform activities that access sensitive data, create or modify user accounts, manage audit policies or export data. Using named accounts allows you to know exactly who performed these actions.

## How does Oracle Database Vault's separation of duty controls work for smaller organizations?

Oracle recommends separate administrators for the additional roles that Oracle Database Vault provides (Oracle Database Vault owner—the security administrator responsible for the security controls and Oracle Database Account Manager—the security administrator responsible for creating and managing new users and profiles). These are separate and distinct from the database administrators. However, in smaller organizations, this may not be possible. In these cases, one or more of these roles may be assigned to the same person.

Similar to how the industry no longer logs in to the operating system as *root* or *Administrator*, Oracle recommends adopting a least privilege model for day-to-day named accounts. Instead of granting all privileges to a named account, you can grant critical roles and privileges to a schema-only account and proxy as if you are that. When you need to use the account, you use the proxy method (e.g. jsmith[high_priv_user]@pdb1). When you need to perform routine actions, you use your account without the proxy method (e.g., connect jsmith@pdb1). If an attacker is able to compromise your named account, they must also know that the critical roles and privileges require the use of proxy authentication. This may not be a significant barrier but it is an additional step an automated attack may not be able to adapt to.

### Can the Oracle Database Vault owner view data that is protected by a realm?

No. The Oracle Database Vault owner can only set up security policies, such as realms and command rules, but cannot see data protected by a realm or a command rule. They cannot grant this access right to themselves.

### Can the security responsibilities of the Oracle Database Vault owner be delegated?

A Database Vault policy can group related realms and command rules and be delegated to a policy owner. The policy owner can update the policy without having the full role and privileges of a Database Vault administrator. The policy owner needs the DV_POLICY_OWNER role to update the policy they are delegated.

### How are changes made by the Oracle Database Vault owner to security objects audited?

All changes made to security objects (enable, disable, add objects, add authorization….) are audited. This cannot be disabled.

### Can Oracle Database Vault block common users from accessing sensitive data in Pluggable Databases?

Starting in Oracle Database 19c Release, Database Vault operations control can block common users (infrastructure DBAs, for example) from accessing local data in pluggable databases (PDBs) in autonomous, regular Cloud, or on-premises environments. Common users and applications that must access PDB local data can be added to an exception list.

### How complex is it to enable Oracle Database Vault operations control?

It is simple to enable and transparent for PDB users. Once Database Vault has been enabled on the CDB, to enable Database Vault operations control you will use the DBMS_MACADM.ENABLE_APP_PROTECTION PL/SQL procedure. There is no need to restart the CDB or PDB databases and Oracle Database Vault does not need to be enabled in the PDB to take advantage of the security that Oracle Database Vault operations control provides.

### Can Oracle Database Vault be managed through Oracle Enterprise Manager?

Yes. Oracle Enterprise Manger Cloud Control provides a management interface for most Oracle Database Vault features, including realms, rules and rule sets, command rules, and more.

### How do Oracle DBA tasks change with Oracle Database Vault?

Most DBA tasks remain unchanged with Oracle Database Vault. One area of change is in creating and managing users and profiles. This security-related task can only be done by a user with the DV_ACCTMGR role. Additionally, tasks that can expose sensitive data, like Data Pump and job scheduling, need separate authorization from an account with the DV_OWNER role.

## Deployment

### What is the performance overhead on the database with Oracle Database Vault realms and command rules?

Testing with Oracle E-Business Suite shows Oracle Database Vault realms and command rules have a minimal overhead of less than 2%. Normal database tuning still applies when Oracle Database Vault is enabled.

## How do you move Oracle Database Vault security policies from a development system to a production system?

There are two ways to do this:

1. Oracle Enterprise Manager allows you to move Oracle Database Vault security policies from one Oracle database to multiple other Oracle Databases.
2. Oracle Enterprise Manager also allows you to generate Oracle Database Vault API script from existing security policies. You can then edit and run this API script on any number of target Oracle Databases to create the security policies there.

## How are applications certified and then deployed with Oracle Database Vault?

Starting from Oracle Database 12c Release 2, Oracle Database Vault has a simulation mode where the Oracle Database Vault security controls are checked, but instead of preventing access, it logs policy violations to a simulation log. This allows the customer to run a regression test end-to-end without interruptions from Oracle Database Vault. The simulation log is analyzed at the end of the regression test to see if any adjustments are required in the Oracle Database Vault security controls. Simulation mode is used again when the application is put into production to do a final check-in production before the Oracle Database Vault protections are enabled.

## How do you apply patches in a Database that is protected by Oracle Database Vault?

Database Vault allows for a database patching mode where the database can be patched without disabling Database Vault. In this case, the Security Administrator (user with the DV_OWNER role) grants the DV_PATCH_ADMIN role to a DBA so the DBA can patch the database. Once patching is done, the Security Administrator revokes the DV_PATCH_ADMIN role from the DBA. The DV_PATCH_ADMIN role allows a DBA to patch the database without having access to protected application data.

## How are DBAs prevented from making unauthorized system and session changes in the database?

Command rules allow you to limit what commands can be run in the database. Once enabled, Database Vault has built-in controls for specific ALTER SYSTEM and ALTER SESSION commands. You can adjust the existing controls, and you can create your own command rules to limit other statements, such as ADMINISTER KEY MANAGEMENT, CREATE DATABASE LINK, etc.

## How do I minimize downtime when enabling Oracle Database Vault?

Oracle Database Vault requires restarting the container and any pluggable database you wish to enable it on. Downtime can be minimized by using RAC-rolling enablement, that is, using Oracle Real Application Clusters and enabling it on each individual node. This is similar to the steps you would perform if you were applying a RAC-rolling patch to your Oracle Database.

Downtime can also be minimized if you perform regular Oracle Data Guard switchovers. You can configure Oracle Database Vault on the primary node and then run the enablement step, but do not restart the primary database; instead, restart the standby Oracle Database. Oracle Database Vault will be enabled on the standby and when you perform a switchover from primary to standby, then Oracle Database Vault will be enabled on both databases. While this does not eliminate downtime, it can help you with enablement by "piggybacking" on regular switchover operations.

Oracle GoldenGate can also minimize downtime. If you are familiar with performing a rolling upgrade or rolling patch with Oracle GoldenGate, you can apply the same steps to configure and enable Oracle Database Vault.

## What is new in Oracle Database Vault 23ai?

In Oracle Database 23ai, Oracle Database Vault adds the following capabilities:

- Control authorizations for unified and traditional auditing, allowing you to have tighter control over which privileged users can use the AUDIT_ADMIN and AUDIT_VIEWER roles.
- Control authorization for Oracle SQL Firewall.
- Quickly enable or disable Oracle Database Vault tracing using two new APIs.
- Take advantage of a new function to identify client hosts and IP CIDR ranges in rules.
- Specify fewer parameters when creating or updating realms, command rules, realms, rules, and factors.

# More Information

## Where can I find more information on Oracle Database Vault?

For more information, please see the documentation:

- Oracle Database Vault Getting Started Guide at https://docs.oracle.com/en/database/oracle/oracle-database/23/dvgsg/index.html
- Oracle Database Vault Administrator's Guide at https://docs.oracle.com/en/database/oracle/oracle-database/23/dvadm/index.html.

A variety of helpful information is available online, including a datasheet, technical paper, customer references, end-user documentation, and a discussion forum. Oracle University offers a training course on Oracle Database Vault. https://www.oracle.com/security/database-security/database-vault/

Connect with us.

Call +**1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at: **oracle.com/contact**.

blogs.oracle.com facebook.com/oracle twitter.com/oracle